UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,678	09/28/2001	John R. Fredlund	82616SLP	5488

7590 09/07/2005

Thomas H. Close
Patent Legal Staff
Eastman Kodak Company
343 State Street
Rochester, NY 14650-2201

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,678	FREDLUND ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-43 have been considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3,7-9,11-13,15-18,30-34, and 37-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Cromer, U.S. Patent Application Publication No. 2002/0083323.

As per claim 1, the applicant describes a method of processing for later authentication a digital still image captured using a digital image capture device, comprising the following steps which are anticipated by Cromer:

a) transmitting signature data from a remote location to the digital image capture device [0018];

b) associating an image identification with the captured digital still image [0018];

c) applying the signature data to the captured digital still image to produce an authentication signature representative of the captured digital still image [0018];

d) associating the authentication signature with the image identification [0018];

e) transmitting the authentication signature to the remote location ([0024] and [0026]);

f) storing the signature data, authentication signature, and image identification at the remote location ([0024] and [0026]);

Regarding parts e) and f), the information transmitted to the remote location includes the image, the camera's digital signature, and the photographer's digital signature [0022]. Once the data is received, it is stored in a system, such as a system for Sport's Illustrated [0026], and authentication can take place at anytime [0024] and [0025].

As per claims 2,3, and 18, the applicant describes the method of claims 1 and 16, which are met by Cromer (see above), with the following limitation which is also met by Cromer:

Further comprising the step of capturing the digital still image after the signature data is transmitted to the digital image capture device from the remote location [0018].

As per claim 7, the applicant describes the method of claim 1, which is met by Cromer (see above), with the following limitation which is also met by Cromer:

Further comprising the step of associating the signature data with the image identification [0018];

As described by Cromer, "the digital signature and information related to the user is associated with the captured image" [0018]. The image identification could also be the image itself, which is sent alongside the camera's digital signature and the photographer's digital signature [0022].

As per claim 8, the applicant describes a method of authenticating a digital still image captured using a digital image capture device and processed using signature data to produce an authentication signature wherein the authentication signature is stored at a remote location for later use in verifying the authentication of the captured digital still image, comprising the following limitations which are met by Cromer:

a) transmitting the digital still image to the remote location [0024];

b) accessing the signature data [0024];

c) applying the signature data to the transmitted digital still image to produce a verification signature [0024];

d) accessing the authentication signature stored at the remote location, and

e) comparing the authentication signature with the verification signature to determine the authentication of the transmitted digital still image [0024].

As per claims 9,13,17,32, and 34, the applicant describes the method of claims 8,12,16,30, and 33, which are met by Cromer (see above), with the following limitation which is also met by Cromer:

Further comprising the step of producing an authentication message indicative of the authentication of the digital still image [0024];

Since one is able to determine the camera used and whether the photograph has been altered, it is inherent that a message is sent to the user.

As per claim 11, the applicant describes the method of claim 8, which is met by Cromer (see above), with the following limitation which is also met by Cromer:

Further comprising the step of verifying the authenticity of the signature data [0024].

As per claim 12, the applicant describes a method of authenticating a digital still image having an image identification and captured using a digital image capture device and processed using signature data to produce an authentication signature wherein the authentication signature, signature data, and image identification is stored at a remote location for later use in verifying the authentication of the captured digital still image comprising the following limitations which are met by Cromer:

a) transmitting an authentication request for the digital still image ([0024] and [0026]);

b) determining the image identification for the digital still image to be authenticated [0019];

c) determining, from the remote location, the signature data and authentication signature associated with the image identification ([0024] and [0026]);

d) transmitting the signature data from the remote location to an authentication location remote from the remote location ([0019] and [0026]);

e) applying the signature data to the digital still image to be authenticated at the authentication location to produce a verification signature [0021];

f) transmitting the verification signature from the authentication location to the remote location [0024];

g) comparing the authentication signature and the verification signature to determine the authentication of the digital still image [0024];

The authentication location is the digital image capture device and the remote location is the system, such as the Sport's Illustrated system, which accepts the transmitted image and signatures and determines authenticity. The verification signature is one of the two signatures sent by the digital image capture device. The authentication signature is the hash of the image calculated at the remote location. Since the authentication signature is compared with the verification signature after the authentication signature is calculated [0024], it is first stored in memory before it is used to authenticate an image.

As per claim 15, the applicant describes the method of claim 12, which is met by Cromer (see above), with the following limitation which is also met by Cromer:

Wherein the authentication location is the digital image capture device or a personal computer [0018];

The authentication location is the digital image capture device.

As per claim 16, the applicant describes a method of authenticating a digital still image captured using a digital image capture device comprising the following limitation which are met by Cromer:

a) transmitting signature data from a remote location to the digital image capture device [0019];

b) associating an image identification with the digital still image [0020];

c) applying the signature data to the captured digital still image to produce an authentication signature representative of the captured digital still image [0018];

d) associating the authentication signature with the image identification [0018];

e) transmitting the authentication signature to the remote location [0024];

f) storing the signature data, authentication signature, and image identification at the remote location [0024];

g) transmitting the digital still image to the remote location [0024];

h) accessing the signature data for the transmitted digital still image [0024];

i) applying the signature data to the transmitted digital still image to produce a verification signature [0024];

j) comparing the authentication signature with the verification signature to determine the authentication of the transmitted digital still image [0024].

As per claim 30, the applicant describes a system for processing for later authentication a digital still image, comprising the following limitations:

a) a digital image capture device for capturing the digital still image [0018];

b) a remote location remote from the digital image capture device comprising a database for storing signature data, an authentication signature, and an image identification, the image identification being associated with the digital still image captured by the digital image capture device, and the authentication signature being associated with the image identification [0024];

c) communication means for transmitting the signature data from the remote location to the digital image capture device, and transmitting the authentication signature from the digital still image to the remote location ([0019] and [0024]);

d) an image processor disposed in the digital image capture device for applying the signature data to the captured digital still image to produce the authentication signature, the authentication signature being representative of the captured digital still image [0021];

Regarding part d), it is inherent in the art that the digital image capture device comprises a processor in order to apply the signature data and transmit the data to the remote location.

As per claim 31, the applicant describes the system of claim 30, which is met by Cromer (see above), with the following limitation which is also met by Cromer:

Wherein the signature data comprises a hashing algorithm [0021].

As per claim 33, the applicant describes a system for authenticating a digital still image captured using a digital image capture device and processed using signature data provided to the digital image capture device to produce an authentication signature representative of the digital still image comprising the following limitations:

a) a remote location remote from the digital image capture device comprising a database for storing the signature data and authentication signature [0024];

b) communication means for transmitting the digital still image to the remote location for authentication [0024];

c) a processor located at the remote location for applying the signature data to the transmitted digital still image to produce a verification signature and comparing the authentication signature with the verification signature to determine the authentication of the digital still image [0024];

Regarding part c), it is inherent that the remote location comprises a processor for performing the functions described in paragraph [0024].

As per claim 37, the applicant describes a digital still image processed according to the method of claim 1 [0018].

As per claim 38, the applicant describes a computer storage product having at least one computer storage medium having instructions stored therein causing one or more computers to perform the method of claim 1 [0016].

As per claim 39, the applicant describes a computer storage product having at least one computer storage medium having instructions stored therein causing one or more computers to perform the method of claim 8 [0016].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer, U.S. Patent Application Publication No. 2002/0083323.

As per claim 4, the applicant describes the method of claim 1, which is met by Cromer (see above), with the following limitation:

Wherein the signature data from the remote location is transmitted to the digital image capture device subsequent to the capture of the digital still image ([0021] to [0022]);

Cromer discloses that the signature data, such as which public/private key to use, is sent to the digital image capture device before the image is taken in the preferred embodiment. However, the process of Cromer's system as described in paragraphs [0021] and [0022] is one in which first an image is captured, second a digest is created using the image and the digital signature of the camera, and third the digest is encrypted using the photographer's private key. Furthermore, the information about the photographer which is obtained from the RF interface [0020] is not used until after the image has been captured and a digest has been created using the image and the camera's digital signature. This means that the signature data could be transmitted between the first and third steps (after the image is captured and before the digest is signed using the private key of the photographer) and the system would function the exact same way.

Since the system would function in the exact same way whether the signature data is transmitted before the image is captured or right after the capture of the image, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to transmit the signature data from the remote location subsequent to the capture of the digital still image.

Claims 10 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of Schneier (Schneier, Bruce. Applied Cryptography. 1996. John Wiley and Sons, Inc. Page 56).

As per claims 10 and 14, the applicant describes the method of claims 9 and 13, which are met by Cromer (see above), with the following limitation which is met by Cromer:

Further comprising the step of transmitting an authentication code to verify the authentication of the authentication message;

Cromer discloses all the limitations of claims 9 and 13 (see above). However, Cromer fails to disclose the limitation of transmitting an authentication code, such as encryption, in order to verify that the authentication message is coming from a trusted source.

Schneier discloses that encryption, such as secret key encryption, allows an authentication message to be authenticated by the receiver. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Cromer and incorporate the use of encryption to authenticate the sender of an authentication message.

Claims 5,19,21-25,27-29,35-36, and 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of Kaplan, U.S. Patent Application Publication No. 2002/0023220.

As per claims 5 and 19, the applicant describes the method of claims 1 and 16, which are met by Cromer (see above), with the following limitation which is met by Kaplan.

Wherein the remote location comprises a database for storing the authentication signature (Kaplan: Abstract; [0056]);

See the rejection for claim 21 below.

As per claims 21,27, and 35, the applicant describes a method of authenticating a digital still image captured using a digital image capture device comprising the following limitations which are met by Cromer in view of Kaplan:

a) transmitting signature data from a remote location to the digital image capture device (Cromer: [0019]);

b) associating an image identification with the captured digital still image (Cromer: [0020]);

c) applying the signature data to the captured digital still image to produce an authentication signature representative of the captured digital still image (Cromer: [0018]);

d) associating the authentication signature with the image identification (Cromer: [0018]);

e) transmitting the authentication signature to the remote location (Cromer: [0024]);

f) storing the signature data, authentication signature, and image identification at the remote location (Cromer: [0024]);

g) initiating an authentication request from an authentication location remote from the remote location, the digital still image to be authenticated being disposed at the authentication location (Kaplan: [0056] and [0059]);

h) transmitting the signature data to the authentication location (Kaplan: [0072]);

i) applying the signature data to the digital still image to be authenticated at the authentication location to produce a verification signature (Kaplan: [0072]);

j) transmitting the verification signature to the remote location (Kaplan: [0072]);

k) comparing, at the remote location, the authentication signature with the verification signature to determine the authentication of the transmitted digital still image (Kaplan: [0061] and [0062]);

Parts a) through f) are rejected by Cromer under the rejections as described in the rejection for claim 1. Cromer fails to meet all the limitations of the above claim because Cromer's system fails to describe having both the verification signature and the authentication signature transmitted into the remote location. In Cromer's system, the remote location accepts a signature from a digital image capture device and then calculates a second signature from the received image for comparison and authentication purposes. The above claim is met through the use of a digital image capture device which

calculates and transmits an authentication signature and an authentication location (which could be the digital image capture device) which calculates and transmits a verification signature.

Kaplan describes a system similar to the applicant's system and Cromer's system in which a hash of an image from a source such as a still digital camera [0063] is registered in a witness storage database so that the image can be authenticated at a later time by rehashing the image and comparing the rehash with the original hash stored in the witness server or witness servers. The user-registrant may or may not be the creator of the image [0056]. In the case where the user-registrant is not the creator of the image, the image is transmitted, copied, or sent to a user-registrant who is at the authentication location.

In regards to a request to authenticate an image that the user-registrant has in his possession (part g), the witness server database sends the program or tools necessary to provide a CHF to the user-registrant (part h), who applies the signature data or hash function data to the image to produce a verification signature (part i) which is transmitted to the witness server either as an initial hash storage entry or a second hash (part j). If the verification signature is a second hash, the witness server compares the stored hash with the second hash to determine whether the image is authentic (part k).

Incorporating the ideas of Kaplan and Cromer would involve keeping parts a) through f) the same as described in the rejection for claim 1 in which a digital image capture device captures an image, hashes the image, and sends the image to a remote location system where it is stored and authentication can take place. Adding Kaplan to Cromer's ideas would simply mean that a third party (or the digital image capture device itself) that receives the image captured in Kaplan and Cromer's systems could authenticate the image through the remote location of Cromer by obtaining signature data, as described by Kaplan, and calculating its own hash and then sending the hash to the remote location for authentication verification.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Kaplan and Cromer because by adding the ideas of Kaplan to Cromer authentication of an image can take place by a number of third parties (or by the digital image capture device itself) through a central remote location which provides the appropriate signature data. Though

authentication of the images can take place at the third party locations in Cromer's system, Kaplan's ideas in Cromer is an obviously more efficient system because having a central location where authentication is accomplished is more efficient because such things as signature data could change and an administrator could more easily contact the central location than all the third party locations where authentication is taking place if the third parties receive the signature data before it is changed.

Regarding claim 27, the applicant discloses the system as described above where the authentication location is the digital image capture device. The authentication location can be the digital image capture device since the user who has the digital image at the authentication location can also be the author of the image. A digital image capture device is listed as a possible image creator [0063].

As per claim 22, the applicant describes the method of claim 21, which is met by Cromer in view of Kaplan (see above), with the following limitation which is also met by Kaplan:

Further comprising the step of transmitting the digital still image to be authenticated to the authentication location (Kaplan: [0056]);

As per claims 23, 29, and 36, the applicant describes the method of claims 21,27, and 35, which are met by Cromer in view of Kaplan (see above), with the following limitation which is also met by Kaplan:

Further comprising the step of producing an authentication message indicative of the authentication of the transmitted digital still image (Kaplan: [0056], [0061], and [0062]);

It is inherent in the art that a message of authentication is produced for the user because the whole point of the system is for the user to be able to know whether an image is authentic.

As per claim 24, the claim is rejected on the same grounds as claim 2. Claim 24 is rejected under 103(a) instead of 102(e) because claim 24 depends on claim 21 which is rejected under 103(a).

As per claim 25, the applicant describes the method of claim 21, which is met by Cromer in view of Kaplan (see above), with the following limitation which is met by Kaplan:

Wherein the authentication location is a digital image capture device or a computer (Kaplan: [0056] and [0063]);

As described by Kaplan, the authentication location can be either a digital image capture device in the event that the image generating device is a still digital camera [0063] and the user-registrant is the author of the image [0056], or the authentication location can be a third party which receives the image on a system, such as a computer system, by receiving a transmission of the image or copying the image.

As per claim 28, the applicant describes the method of claim 27, which is met by Cromer in view of Kaplan (see above), with the following limitation which is also met by Kaplan:

Further comprising the step of, prior to transmitting the signature data from the remote location to the digital image capture device, transmitting an authentication request for the digital still image to the remote location from the digital image capture device [0059];

The examiner assumes that transmitting the signature data from the remote location to the digital image capture device refers to the second instance of the signature data being transmitted (part g). As described by Kaplan, a user-registrant, such as a user operating a digital image capture device in one instance (see the rejection for claim 21) contacts the remote location or witness server (where the authentication comparison takes place) with an authentication response. In response, the user operating a digital image capture device is sent the signature data or cryptographic hash function (CHF) and "the user registrant could perform the CHF transformation to obtain the DFP" [0059].

As per claim 42, all of the limitations of the claim are met by the rejection for claim 1, which is met by Cromer (see above), except for the following limitation which is met by Cromer in view of Kaplan:

f) storing the first time, second time, signature data, authentication signature, and image identification at the remote location (Cromer: [0024] and Kaplan: [0035]);

Cromer discloses the use of storing signature data, the authentication signature, and image identification at the remote location [0024]. Cromer also discloses the use of storing the first time at the remote location because discloses incorporating time/date information into the image identification information which is transmitted to the remote location and stored for authentication purposes [0014]. Having the time/date information refer to the instance when the image is captured and the authentication signature is produced. However, Cromer fails to disclose the use of calculating or storing a second time.

The second time in the applicant's system is the time when the image is transmitted to the remote location. Cromer makes no mention of time-stamping an image or calculating a transmission time for an image. However, Kaplan discloses the use of time-stamping a received image. In Kaplan's system, time-stamping an image and storing the time-stamp information is useful in the system as a means to authenticate an image by its receipt time.

Combining Cromer and Kaplan, the limitations of the claim are met because Cromer discloses the use of storing the first time (time image is captured/ authentication signature is calculated), signature data, authentication signature, and image identification, and Kaplan discloses the use of storing the second time (time image is transmitted). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Kaplan with those of Cromer and add the use of storing a second time, or time-stamp the image is sent, at the remote location because doing so would add a further method for authenticating the image at the remote location.

As per claim 43, the applicant describes the method of claim 42, which is met by Cromer in view of Kaplan (see above), with the following limitation which is also met by Cromer in view of Kaplan:

Wherein the first and second time are determined by the digital image capture device;

The first and second time are determined by the digital image capture device. In Cromer's system, the first time is determined when the user takes the image and incorporates the signature data. In Kaplan's system, the second time is also determined by the digital image capture device. The time-stamp, or time the image is sent, is applied at the receiving remote location in Kaplan's system, but it is the digital image capture device which determines when the image is transmitted and when the image is sent.

Claims 6,20, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of Lambert, U.S. Patent Application Publication No. 2001/0007128.

As per claims 6,20, and 26, the applicant describes the method of claims 1,16, and 21, which are met by Cromer (see above), with the following limitation which is met by Lambert:

Further comprising the step of transmitting a message indicative of receipt of the authentication signature by the remote location (Lambert: [0039]);

Cromer describes all the limitations of independent claims 1 and 16. However, Cromer fails to describe the step of transmitting a receipt message from the remote location when the authentication signature has been received by the remote location.

Lambert describes a secure communication method in which one system sends a second system a receipt message when it has received data from the second system (Lambert: [0039]). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Lambert with those of Cromer and add the use of transmitting a receipt message once data has been received so that a sending system can be sure that the receiving system has received the data for the purpose of security and for the purpose of knowing that the sending system doesn't have to resend the data.

Claims 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cromer in view of Friedman, U.S. Patent No. 5,499,294.

As per claims 40 and 41, the applicant describes a method of processing for later authentication a digital still image captured using a digital image capture device, comprising the limitations of claim 1, which is met by Cromer (see above), with the additional limitation that the additional limitation of segmenting the captured digital still image which is met by Friedman (Col 8, lines 53-67).

Friedman describes a system where a digital camera captures images and streams of images and partitions the captured data into blocks. The blocks of data are then encrypted with signature data and transferred into a storage medium.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Friedman with those of Cromer and segment data in order to facilitate the processing of data.

Response to Arguments

Applicant's arguments filed 8/22/05 with respect to claim 1 have been fully considered but they are not persuasive. The applicant presents five arguments.

Regarding 1, the applicant argues part a. More specifically, the applicant argues that Cromer does not teach "transmitting signature data from a remote location to the digital image capture device". Cromer discloses a digital image capture device which is unique in that it has a RF interface for receiving information from and communicating information to a remote location. Among the information received from a remote location is information used in the computation of a signature ([0018], [0019]).

Regarding 2, the applicant argues part c. More specifically, the applicant argues that Cromer has additional functionality such as creating a second digital signature out of a digest computed from a first digital signature and an image. The argument that Cromer has additional features is irrelevant to the claimed invention. Cromer teaches part c as signature data, received through an RF interface, is integrated with the image before a digest is formed [0021]. The applicant further argues that "the claimed invention uses a hashing algorithm modified by signature data to hash the image" (Remarks, page 3). Nowhere in the claimed invention of claim 1 does the applicant require a hashing algorithm, let alone a hashing algorithm modified by signature data. Further, the examiner fails to see how the statement that the invention "uses a hashing algorithm **modified by** signature data" is consistent with the Specification.

Regarding 3 and 4, the applicant argues that Cromer does not transmit authentication data outside of the camera. This statement is not consistent with Cromer. Cromer discloses the use of an RF interface to exchange data with a remote location so that an image can be later verified. In one

embodiment, a remote location may be the photographer's company, such as Sports Illustrated. Further, the RF interface is equipped with the public key of Sports Illustrated so that the captured image is encrypted with the public key, transmitted to Sports Illustrated, and only viewed at Sports Illustrated by decrypting with the complimentary private key [0026]. Similarly, it is possible to ascertain which camera a received image came from by retrieving the stored public key of the given camera, decrypting the signature, and comparing the hash with a newly-generated hash to determine if the received image came from the camera it was supposed to come from:

"If they [the hashes] are equal, the photograph is a non-modified original that came from the given camera. If they are not equal, the photograph is altered and the camera used cannot be determined or validated" [0024].

The applicant's statements that this process takes place internally within a camera is not consistent with the primary reference. If the authentication did take place within the camera, there would be no point or reason for determining which camera was used because the stored images all would come from the same camera. In contrast to the applicant's statements, Cromer teaches performing authentication to validate that a picture received at a remote location was captured by one of a plurality of cameras.

Regarding 5, the applicant presents another argument which is outside the scope of the claims. Again, the fact that Cromer may have additional features does not preclude Cromer from meeting the limitations of the applicant's claimed invention.

Applicant's arguments with respect to claim 12 have been fully considered but are not persuasive. The applicant argues that there is no mention of encryption in claim 12 so Cromer cannot be applied. This argument is considered moot because nowhere in claim 12 does the applicant preclude the use of encryption.

Applicant's arguments with respect to the 103 rejections have been fully considered but are not persuasive. The applicant argues that the claimed invention does not include encryption and the

combinations are therefore not obvious. Again, the examiner notes that the claimed invention does not preclude the use of encryption.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

E. Moise

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER